IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	4:11CR3019
	)	
v.	)	
	)	FINDINGS, RECOMMENDATION,
ROBERT F. RIGHTER,	)	AND ORDER
	)	
Defendant.	)	

The defendant has filed a motion to suppress all evidence obtained during the search of his residence located at 500 Surfside Drive, #33, Lincoln, Nebraska. (Filing No. 13). The search was conducted on January 14, 2011 pursuant to a warrant issued on January 13, 2011 by Lancaster County Court Judge Susan Strong. (Filing No. 18). During the search, three computers and three hard drives, among other items, were seized from defendant's apartment. He was arrested for receiving or distributing child pornography.

The defendant claims the evidence obtained during the search must be suppressed because the warrant application, on its face, fails to support a finding of probable cause. (Filing No. 15). The defendant does not claim the affiant officer made false statements or concealed material information when presenting the warrant application, or that the issuing judge "rubber-stamped" the warrant.

The warrant application and warrant were filed for the court's review. (Filing No. 18). After reviewing these documents, and for the reasons stated below, the defendant's motion to suppress should be denied without a hearing.

STATEMENT OF FACTS

The affiant officer, John C. Donahue, is an Investigator for the Lincoln, Nebraska Police Department, and has been a Certified Law Enforcement Officer since 1986. As set forth in detail in the warrant affidavit, Investigator Donahue has extensive experience and training in forensic computer examinations and computer crime investigations, including the use of peer-to-peer (P2P) file-sharing networks to commit computer crimes.

Based on this training and experience, Investigator Donahue's warrant affidavit explains:

- Computer users can chose to install publicly available P2P software which facilitates the trading of digital files between computer users.

- P2P software connects a computer user, a "peer," to a computer designated by the software to serve as an index server, (an "ultra-peer"). Ultra-peer computers, in turn, connect with other ultra-peer computers to share index lists of available files.

- A peer can search for digital files by submitting text containing search terms to the ultra-peer. The ultra-peer searches its own files for the terms, and also sends the search terms to other ultra-peers which, in turn, examine their index list of files. If files responsive to the search are located, the requesting peer receives information from the ultra-peer on how to connect to peers with files available for sharing. The requesting peer can then choose to download files directly from other peers, and can choose to receive the responsive files from only one source or several. Provided several files were, at one time, all part of one original file, by selecting numerous sources, the requesting peer can obtain a complete

original. The P2P software will balance the network load, accept pieces of the original file from different users, and reassemble the file at the peer's local computer.

- In accordance with developments implemented by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), digital files are assigned a Secure Hash Algorithm Version 1 (SHA1) compressed digital representation resulting in a digital signature assigned to each file. By comparing these signatures, Investigator Donahue can determine if two files are, or are not, identical with a precision that exceeds 99.9999 percent certainty even if file names have been changed. The use of SHA1 compressed digital representations to match movies and images is extremely reliable.

- Peer users attempting to trade files on a P2P file-sharing network can place files from their local computer in a shared file directory, and if the peer starts the P2P software, the local computer calculates the SHA1 signature for each shared file and provides the information to other users wishing to trade files.

- Law enforcement agencies have compiled a list of SHA1 digital signatures for many child pornography images, and use this information to conduct undercover operations involving images, video, or text files of child pornography being traded on P2P networks. When conducting this type of investigation, Investigator Donahue enters search terms in the P2P software, and receives a list of SHA1 digital signatures of responsive images available for download. If a digital signature corresponds to a known child pornography file, he submits a download request for the file.

- Internet computers identify each other by an Internet Protocol or IP address which can, in turn, assist law enforcement officers to find the computer's internet service provider (ISP). Using the date and time the IP address was used, law enforcement can then obtain information from the service provider which identifies the account holder by name and the physical address of the computer.

- By examining a list of IP addresses, Investigator Donahue can locate computers reportedly in Nebraska. By comparing SHA1 digital signatures to IP addresses, he can determine that a computer with P2P software originating from an IP address in Nebraska contains images of child pornography. Using this information, the internet service provider can identify the specific physical address of the computer.

- During an undercover internet investigation, IP address 76.84.231.144 was identified as having files that may contain child pornography available for sharing. Over 100 instances of file-sharing by the automated software occurred between November 19th, 2010, and the date of the warrant, January 13, 2011. In response to an administrative subpoena, Time Warner/Roadrunner identified the account holder for the IP address as Robert Righter, 500 Surfside Drive. Apt 33, Lincoln, Nebraska, 68528-1075.

- As of December 30, 2010, over 300 files were advertised as available from the computer at IP address 76.84.231.144. The warrant application lists, by name, four of these files, and the names listed are highly indicative of child pornography images. Investigator Donahue used P2P sharing software to download the four files from other peer computers on the Gnutella file-sharing network. All four videos were visually reviewed, at least two of which were

reviewed by Investigator Donahue himself. The videos depicted child pornography.

The warrant application requested authority to search the premises at 500 Surfside Dr. Apartment #33, Lincoln, Nebraska for evidence indicative of the crime of possessing and distributing of child pornography, including paper or digital files of such images, computers and computer-related information within the home, and evidence of ownership. A county court judge issued the warrant.

LEGAL ANALYSIS

The defendant claims the warrant application lacks a sufficient probable cause showing because: 1) Investigator Donahue cited no basis for stating a comparison of SHA1 values to known child pornography is 99.9999% accurate in locating files containing child pornography on a computer; 2) without a detailed description of the shared files, the affidavit lacked factual information upon which the issuing judge could independently assess Investigator Donahue's conclusion that files and images constituted child pornography; 3) the files actually viewed were obtained from computers other than the defendant's; 4) Investigator Donahue did not personally view the contents of the four files named in the affidavit, and the person who actually viewed the files was not identified or shown to be reliable; and 5) the information in the affidavit was stale.

A search warrant is valid under the Fourth Amendment if it is supported by probable cause. U.S. v. Stevens, 530 F.3d 714, 718 (8th Cir. 2008). When presented with a warrant application, the court must conduct a "'practical, common-sense inquiry,' consider 'the totality of the circumstances set forth,' and determine if, based on the information in the application, there exists a 'fair probability that contraband or evidence of a crime will be found in a

particular place.'" Stevens, 530 F.3d at 718 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

Investigator Donahue's affidavit describes his training and experience with computer crime investigations, describes the origin of SHA1 values, and explains how law enforcement uses these values to create a master list for digital images known to depict child pornography. The application then states that based on this officer's experience and training, SHA1 values are 99.999% reliable in identifying illegal pornographic images. Contrary to the defendant's argument, Investigator Donahue's affidavit provides ample foundation for his opinions and conclusions regarding the accuracy of SHA1 values and their usefulness in investigating child pornography. U.S. v. Mutschelknaus, 592 F.3d 826, 829 (8th Cir. 2010) (reaffirming an affiant's training and experience in child pornography investigations must be considered when evaluating the sufficiency of a search warrant application).

The warrant application also lists the names of four videos available for sharing from the computer at IP address 76.84.231.144. The computer at this IP address was identified to an account in defendant's name and located at defendant's residence. Even without SHA1 value comparisons and information in the warrant application, the names of these videos alone were indicative of child pornography.[1]

The application vividly describes the contents of the four named videos. Although the defendant argues to the contrary, based on the express statements within the affidavit, Investigator Donahue personally reviewed at least two of the four named videos. These video descriptions not only met, but far exceeded, the level of specificity required to obtain a warrant

[1]The video names included "ANNI 10 Hussyfan) (Pthc) Vicky 7yo and 10yo 69 Pedo Child Porno Lolita.mpg," "preteen pedo (pthc) vicky_9yo_ early works (rare) beautiful 24min.mpg," and "PTHC - beauty-cumshot 3yo THIS ROCKS pedo child toddler incest 2yo 4yo 5yo 6yo 7yo Byo babyj viCKY laura jenny sofie fdsa hussyfan russian korea.mpg."

to search a computer for images depicting sexual exploitation of children. See U.S. v. Grant, 490 F.3d 627, 632 (8th Cir. 2007) (holding an affidavit was sufficient to establish probable cause for issuing a search warrant where the application did not describe the images seen by a computer repairman, but the repairman described the images as disturbing, unlike any he had seen before, and appeared to be "child pornography").

Finally, the defendant claims the warrant application information was stale. As explained by the Eighth Circuit:

> Probable cause must exist when a warrant is issued, not merely at some earlier time, but there is no bright-line test for determining when information is stale. . . . Furthermore, time factors must be examined in the context of a specific case and the nature of the crime under investigation. . . Where continuing criminal activity is suspected, the passage of time is less significant. . .

U.S. v. Morrison, 594 F.3d 626, 631 (8th Cir. 2010)(internal citations and quotation marks omitted).

Investigator Donahue's investigation revealed that over 100 instances of file-sharing by the automated software occurred on the computer at IP address 76.84.231.144 between November 19, 2010, and the date of the warrant application. As of December 30, 2010, only two weeks before submitting the warrant application, the account for IP address 76.84.231.144 was still being used.

Under the totality of the information presented, the information within the warrant application was not stale. Moreover, the application provided a substantial basis for concluding contraband or evidence of child pornography would likely be found during a search of defendant's residence. See, e.g., U.S. v. Stults, 575 F.3d 834 (8th Cir. 2009). The defendant's arguments to the contrary should be denied.

Finally, even assuming this court concluded the warrant application was insufficient, upon review of the application, a state court judge issued a search warrant and the search of defendant's home was conducted pursuant to that warrant. Under the Leon good-faith exception, evidence seized pursuant to a search warrant issued by a judge will not be suppressed "if the executing officer's reliance upon the warrant was objectively reasonable." U.S. v. Proell, 485 F.3d 427, 430 (8th Cir. 2007). Investigator Donahue reasonably relied on the warrant issued by the County Court of Lancaster County as authorizing the search of defendant's home. Defendant's motion to suppress should be denied.

IT IS RECOMMENDED to the Honorable Richard G. Kopf, United States District Judge, pursuant to 28 U.S.C. §636(b)(1)(B), that the defendant's motion to suppress, (filing no. 13), be denied in all respects.

The parties are notified that a failure to object to this recommendation in accordance with the local rules of practice may be held to be a waiver of any right to appeal the district judge's adoption of this recommendation.

IT IS ORDERED: Trial is set for 9:00 a.m. on June 20, 2011 for a duration of three trial days before the Honorable Richard G. Kopf. Jury selection will be at the commencement of trial.

May 19, 2011

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge

*This opinion may contain hyperlinks to other documents or Web sites. The U.S. District Court for the District of Nebraska does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide on their Web sites. Likewise, the court has no agreements with any of these third parties or their Web sites. The court accepts no responsibility for the availability or functionality of any hyperlink. Thus, the fact that a hyperlink ceases to work or directs the user to some other site does not affect the opinion of the court.